

openCRYPT™-SOFT (BS2000/OSD) Version 1.2 Cryptographic basis functions

Issue September 2006

Pages 2

openCRYPT™ products use standardized open interfaces for encryption and decryption.

openCRYPT™ SOFT is an optional integrated solution for cryptographic functions on SX-systems.

It supports, the PKCS#11 based application interface of openCRYPT™-SERV. For SX-systems openCRYPT™-SOFT prepares functions, that are supplied for S-server through the openCRYPT™-BOX.

openCRYPT™-SERV

is based on the PKCS#11 V2.11 interface. The PKCS#11 interface (Public-Key Cryptography Standards#11 (Cryptoki)) is a de facto standard developed by RSA Laboratories in cooperation with security systems developers from industry, universities and government, and provides specifications for accelerating public key encryption and decryption.

Promoted cryptographic algorithms and proceedings

Symmetrical algorithms:

- Block ciphers (DES, DES3,SD2 (≅RC2), AES)
- Operating modes (ECB, CBC)
- Stream ciphers (SD4 (≅RC4))
- Key generation for the supported algorithms

Hash algorithms and integrity codes

MD2, MD5, SHA-1, RIPEMD160, HMAC-MD5, HMAC-SHA-1

Public-key methods

- Cipher/key exchange methods (RSA (PKCS#1), RSA (pure), Diffie-Hellman)
- Signature methods (RSA (PKCS#1), RSA (pure), DSA)
- Key generation for the supported algorithms

Random number generators

Pseudo-random number generators (DES, DES3-OFB)

Methods subject to licensing

In the commercial sector, a license is required for the encryption methods **RC5** and **IDEA**. The licenses for RC5 and IDEA are **not** included in the *openCRYPT* order units. Fujitsu Siemens Computers arranges contact with the relevant rights holders. These functions can be enabled once the licenses have been purchased.

Function-library

The function-library is configured according to the desired application scenario and contains the cryptographic functions for implementing the algorithms listed under *openCRYPT*-SERV.

It corresponds to the *openCRYPT*-BOX-function.

As the base module, it provides the PKCS#11 framework with a modified cryptographic function library using the GNU library of the Hamburg Trust Center (Basis V0.6.1).

The PKCS#11-functions can also be used asynchronous.

Software requirements

OSD/XC V2 or higher
and X2000 V3.0A04 or higher

Hardware requirements

For the arithmetic-intensive cryptographic procedures, at least one additional CPU is necessary for the SX-Systems.

For specifications of the SX-Server please take from the respective system descriptions.

Documentation

The documentation is available in the form of online manuals at <http://manuals.fujitsu-siemens.com> or can be ordered in the form of printed manuals for an additional payment at <http://FSC-manualshop.com>.

Demands on the user

Knowledge of BS2000/OSD cryptographic basis knowledge

Conditions

This software product is supplied to the customer under the conditions for the use of software products against a single payment or installments.

Warranty

Class: A
Delivery format: Machine language

Ordering and delivery

This software product may be obtained from your local Fujitsu Siemens Computers regional office.